

Multi-Factor Authentication Overview

Cardinal requires Multi-Factor Authentication (MFA) to access the **Cardinal Portal** from outside the Commonwealth of Virginia (COV) network. When users log into Cardinal from outside the COV network for the first time, they are prompted to configure MFA. If the user does not select the **do not challenge me on this device again** option, they will be prompted to enter the information based on the authentication option selected when they configured MFA. There are three options available in VITA (Okta) for enabling MFA:

- **SMS Authentication:** Requires you to have a mobile phone registered in the United States or Canada. This function generates a random authentication code and sends a text to your mobile phone (standard text messaging rates apply).
- **Voice Call Authentication:** Requires you to have access to a phone (mobile or land line) registered in the United States or Canada. This function generates a random authentication code and places a call to the phone number set up and the code is verbally stated for entry.
- **Google Authenticator** (not recommended by Cardinal)
Requires you to download the **Google Authenticator** app to your mobile device (must be Apple, Android, or Blackberry) and standard data usage rates apply.

This job aid provides the steps to configure MFA for the options listed above.

We are recommending you utilize a current version of either the Chrome or Internet Explorer browser when accessing Cardinal. If issues are encountered with one of these browsers, try the other browser option. If you experience issues, please submit a Helpdesk ticket via email to VCCC@vita.virginia.gov and include the word **Cardinal** in the subject line of the email.



Security and Access Job Aid


SW SEC: Cardinal Multi-Factor Authentication


Table of Contents

Accessing Multi-Factor Authentication	3
Setting Up SMS Authentication	6
Logging in After Setting up SMS Authentication	11
Setting Up Voice Call Authentication	13
Logging in After Setting up Voice Call Authentication	19
Appendix	21
Setting Up Google Authenticator	21
Barcode – Can't scan	28
Logging in After Setting up Google Authenticator	33

Accessing Multi-Factor Authentication

1. Start by entering the following URL in your computer browser: my.cardinal.virginia.gov.



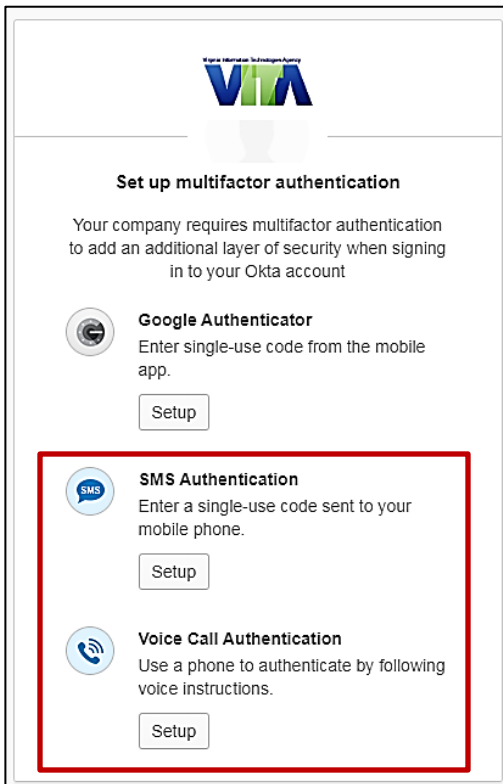


Notice and Warning

This system is the property of the Commonwealth of Virginia. By accessing and using this computer system, you are consenting to system monitoring for law enforcement and other purposes. All activity on this system is monitored. Evidence of unauthorized access, unauthorized use, misuse, or abuse of this system or the information contained in this system shall be promptly reported to appropriate agency management, security personnel, and federal, state, and local law enforcement officials for investigation and criminal prosecution. You will also be subject to all criminal and civil penalties allowed by the law.

[Forgot Username](#) [Forgot Password](#)
[User Registration](#) [Sign-on Help](#)

2. The **Cardinal Login** page displays.
3. Enter your Cardinal Username in the **Cardinal Username** field.
4. In the **Password** field, enter the appropriate password:
 - a. COV users: enter your network password.
 - b. Non-COV users: enter the password you created during the registration process.
5. Click the **Sign In** button.



Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account

Google Authenticator
Enter single-use code from the mobile app.

SMS Authentication
Enter a single-use code sent to your mobile phone.

Voice Call Authentication
Use a phone to authenticate by following voice instructions.

6. When you are outside the Commonwealth of Virginia (COV) network, the **VITA Set up multifactor authentication** page displays.
7. Go to the appropriate section in this job aid based on the authentication method you choose.

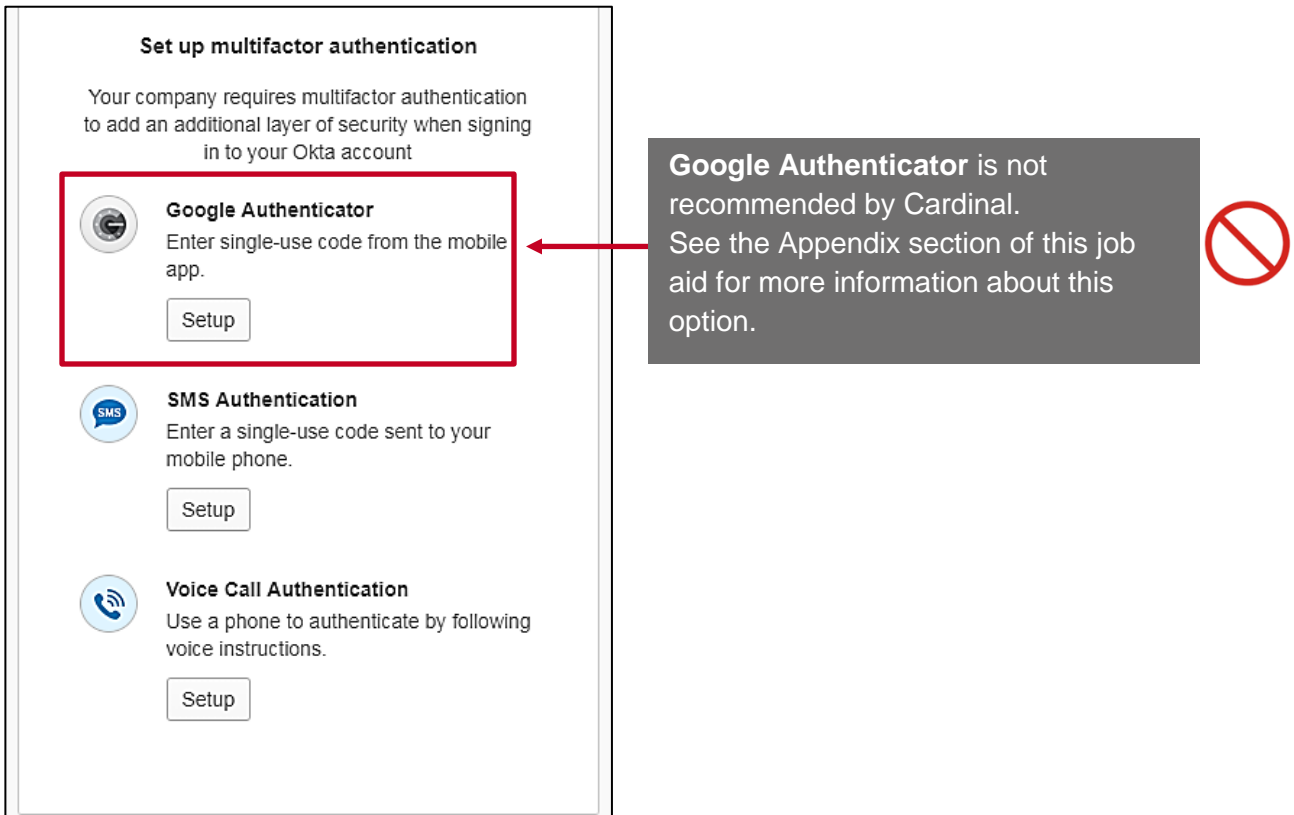
MFA options:

a. [SMS Authentication](#)

- Your mobile phone must be registered in the United States or Canada to select this option.
- A text message is sent to your mobile phone with an authentication code you will need to enter on your computer/device.
- Standard text messaging rates apply.

b. [Voice Call Authentication](#)

- Your phone must be registered in the United States or Canada to select this option.
- Once you enter your phone number (mobile or land line) in the system, a phone call is placed to the number. Once you answer the call, the code is verbally stated twice.
- Enter the code into your computer/device.



Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account

Google Authenticator
Enter single-use code from the mobile app.
[Setup](#)

SMS Authentication
Enter a single-use code sent to your mobile phone.
[Setup](#)

Voice Call Authentication
Use a phone to authenticate by following voice instructions.
[Setup](#)

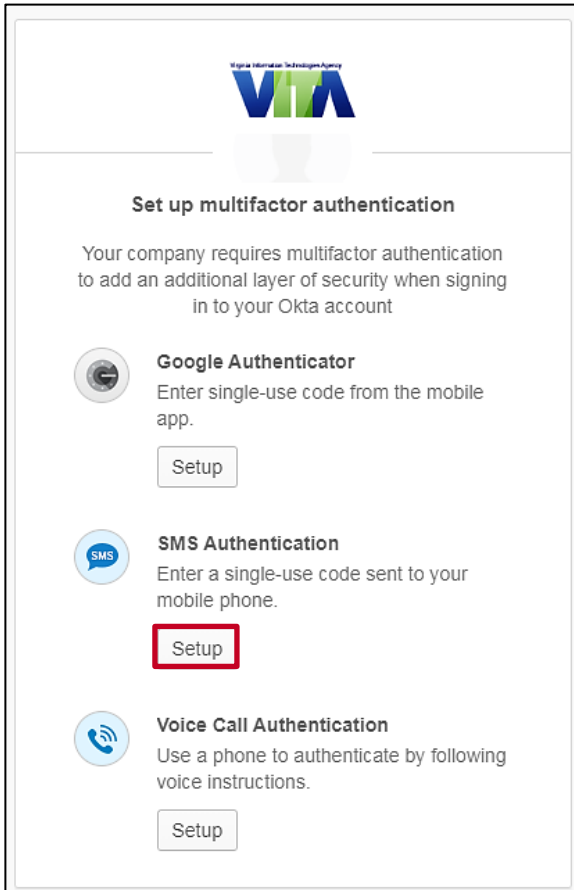
Google Authenticator is not recommended by Cardinal.
See the Appendix section of this job aid for more information about this option.

- c. [Google Authenticator](#) not recommended by Cardinal – see the **Appendix** to use this option)
- You must have an Apple, Android, or Blackberry mobile device.
 - You must download the Google Authenticator app to your mobile device.
 - Standard data usage rates apply.

Note: If you are using an online version of this job aid, click on one of the options above to access that portion of the job aid.

Setting Up SMS Authentication

Receive a One-Time Passcode (OTP) via SMS. A random authentication code is generated on your mobile phone (standard text messaging rates apply). Your mobile phone must be registered in the United States or Canada to select this option.



Set up multifactor authentication

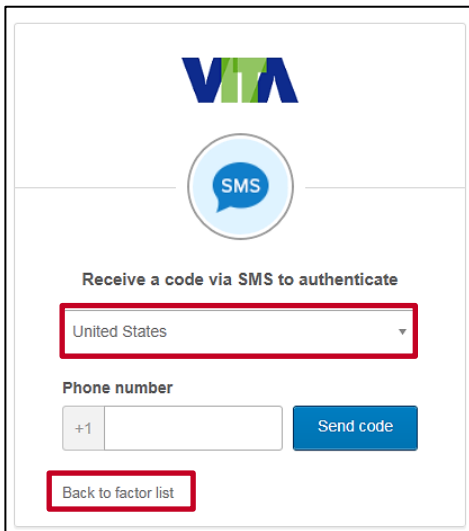
Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account

Google Authenticator
Enter single-use code from the mobile app.

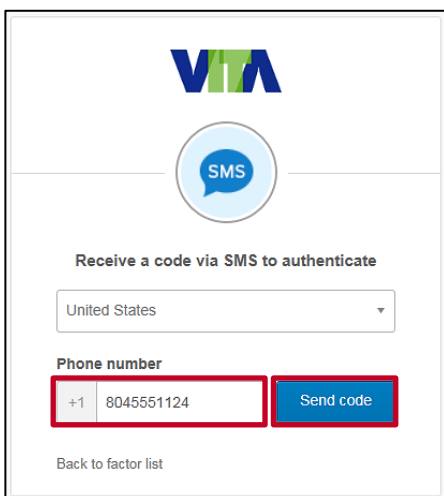
SMS Authentication
Enter a single-use code sent to your mobile phone.

Voice Call Authentication
Use a phone to authenticate by following voice instructions.

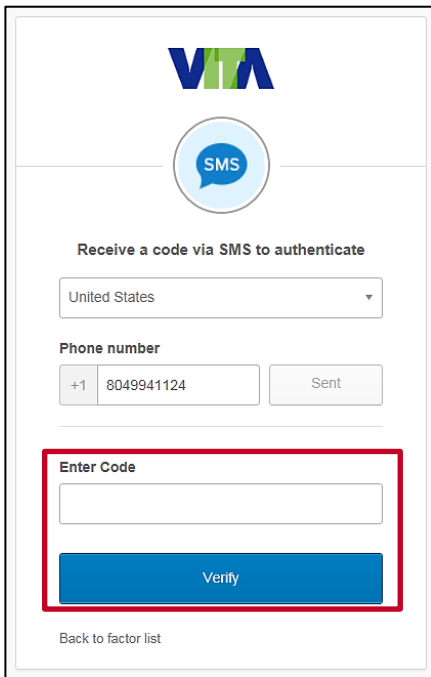
1. Click the **Setup** button under the **SMS Authentication** section of the screen.



2. The **SMS** page displays.
3. In order to use this option, you must have a mobile phone registered in the United States or Canada. **United States** defaults in the country drop-down menu field.
 - a. If your phone is registered in the United States, go to the next step.
 - b. If your phone is registered in Canada, click the drop-down menu, select **Canada**, go to the next step.
 - c. If your phone is not registered in the United States or Canada, click the **Back to factor list** link to return and choose another method for authentication.

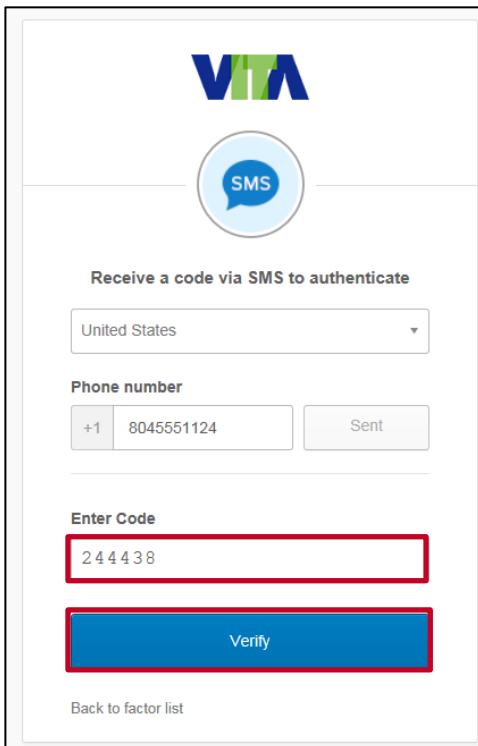


4. Click in the **Phone number** field.
5. Enter your mobile phone number including area code.
6. Click the **Send code** button.



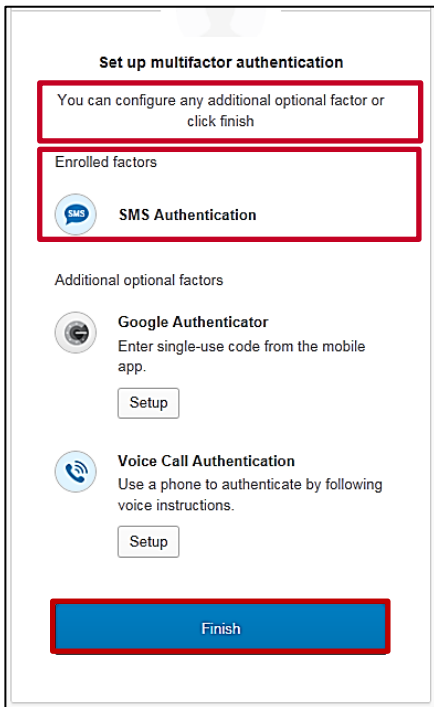
The screenshot shows the Cardinal Multi-Factor Authentication interface. At the top is the VITA logo. Below it is a blue circle with 'SMS' inside. The text 'Receive a code via SMS to authenticate' is displayed. There is a dropdown menu for 'United States'. Below that is the 'Phone number' section with a field containing '+1 8049941124' and a 'Sent' button. The 'Enter Code' field and the 'Verify' button are highlighted with a red box. At the bottom is a link 'Back to factor list'.

7. An **Enter Code** field and **Verify** button display on the page.
8. A text message displays on your mobile phone with the authentication code.



The screenshot shows the Cardinal Multi-Factor Authentication interface. At the top is the VITA logo. Below it is a blue circle with 'SMS' inside. The text 'Receive a code via SMS to authenticate' is displayed. There is a dropdown menu for 'United States'. Below that is the 'Phone number' section with a field containing '+1 8045551124' and a 'Sent' button. The 'Enter Code' field and the 'Verify' button are highlighted with a red box. The 'Enter Code' field now contains the text '244438'. At the bottom is a link 'Back to factor list'.

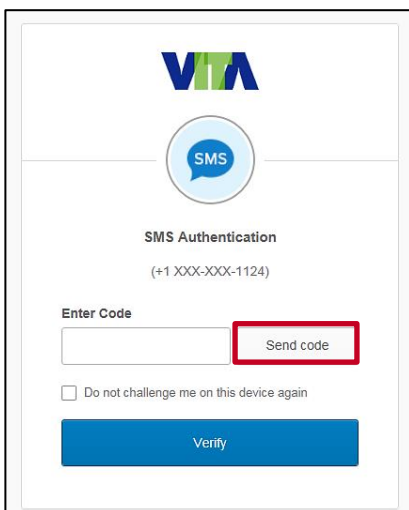
9. Enter the authentication code in the **Enter Code** field on your computer/device.
10. Click the **Verify** button.



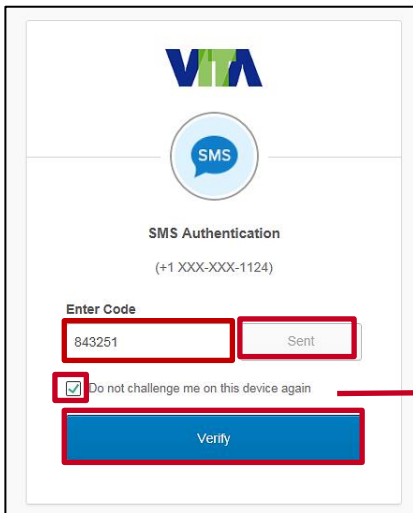
11. The **Set up multifactor authentication** page displays. A message indicates You can configure additional optional options or click finish. The authentication option you selected displays under the **Enrolled factors** section of the page.

Note: If you are using Chrome, you will see a green checkmark next to your enrolled factor.

12. Click the **Finish** button. Now that you have completed your authentication setup, you will be required to authenticate again to log into the Cardinal Portal.



13. The **SMS Authentication** page displays.
14. Click the **Send code** button to send a new authentication code.



Do not select this option if this is a shared computer/device.

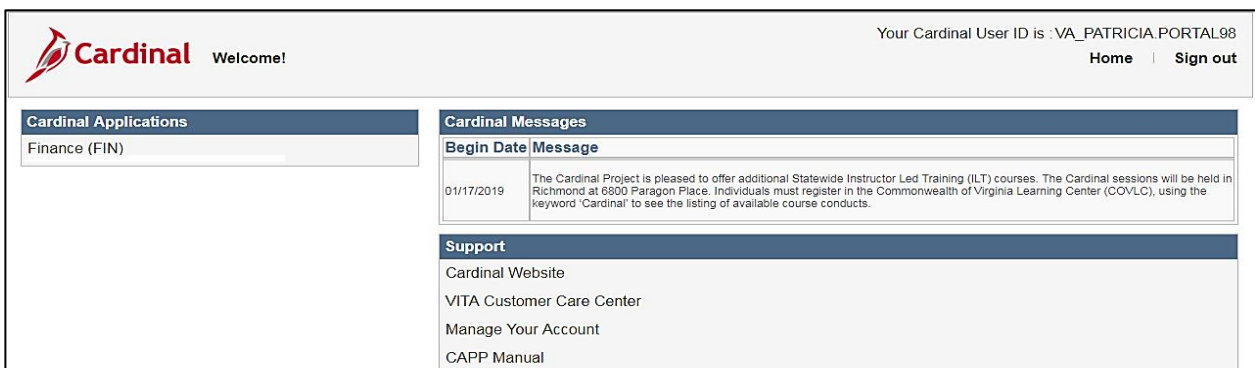
15. The **Send code** button changes to **Sent**.

Note: After about 30 seconds, the **Sent** button changes to **Re-send Code**.

16. An authentication code is sent to your mobile device.
17. Enter the authentication code that displays on your mobile device in the **Enter Code** field on your computer/device.
18. To skip this step in the future, select the **Do not challenge me on this device again** check-box. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

Note: If you clear the browser cache on your computer/device, you will need to enter the authentication code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the authentication code, to have settings added back to the computer/device.

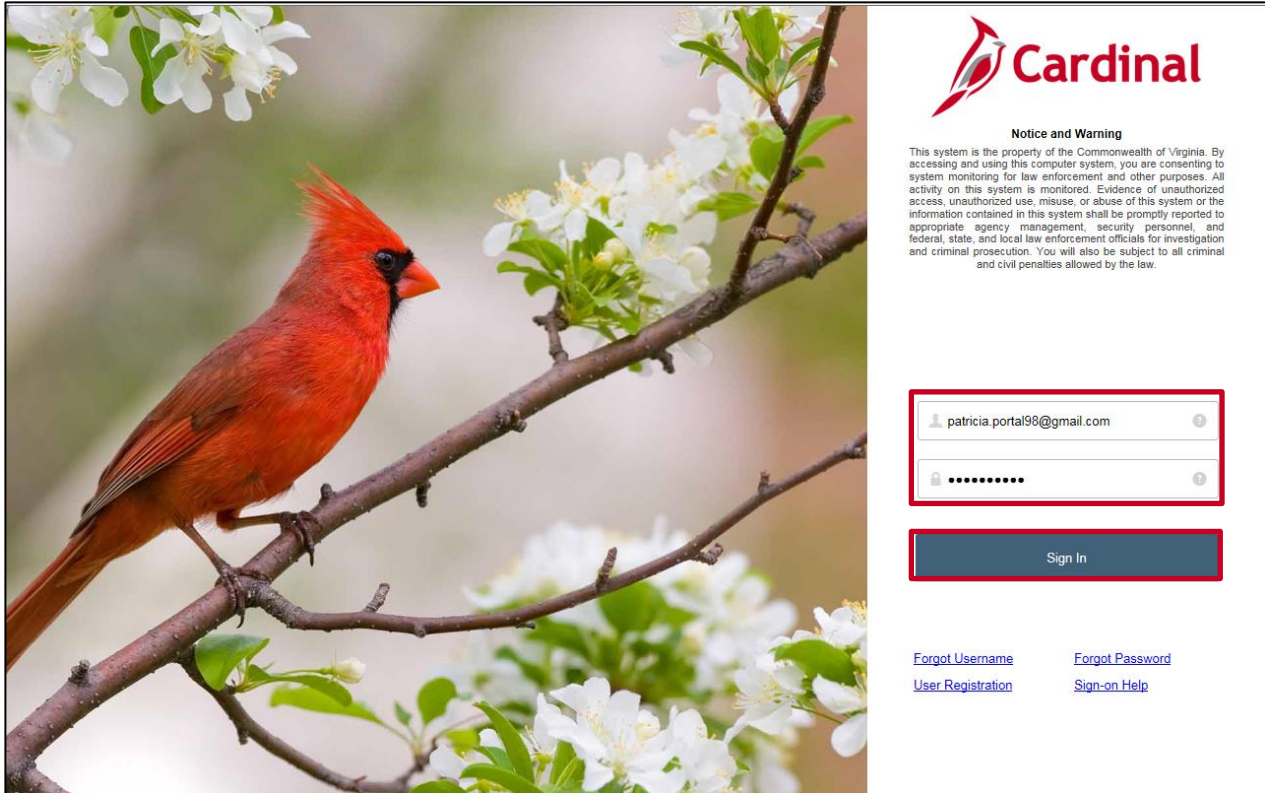
19. Click the **Verify** button to access the **Cardinal Portal**.



20. The **Cardinal Portal** displays.

Logging in After Setting up SMS Authentication

1. Start by entering the following URL in your computer browser: my.cardinal.virginia.gov.



Cardinal

Notice and Warning

This system is the property of the Commonwealth of Virginia. By accessing and using this computer system, you are consenting to system monitoring for law enforcement and other purposes. All activity on this system is monitored. Evidence of unauthorized access, unauthorized use, misuse, or abuse of this system or the information contained in this system shall be promptly reported to appropriate agency management, security personnel, and federal, state, and local law enforcement officials for investigation and criminal prosecution. You will also be subject to all criminal and civil penalties allowed by the law.

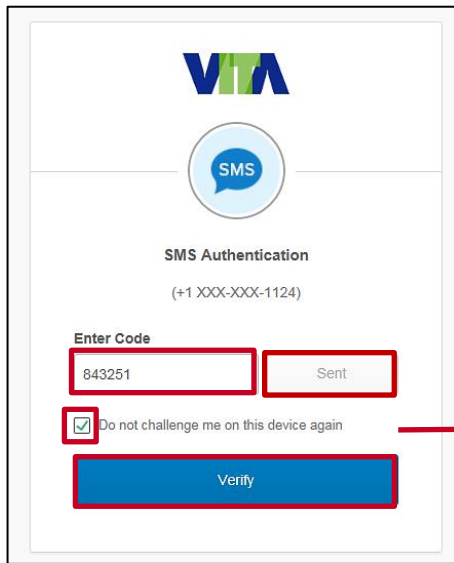
patricia.portal98@gmail.com

.....

Sign In

[Forgot Username](#) [Forgot Password](#)
[User Registration](#) [Sign-on Help](#)

2. Enter your Cardinal Username in the **Cardinal Username** field.
3. In the **Password** field, enter the appropriate password:
 - a. COV users: enter your network password.
 - b. Non-COV users: enter the password you created during the registration process.
4. Click the **Sign In** button.

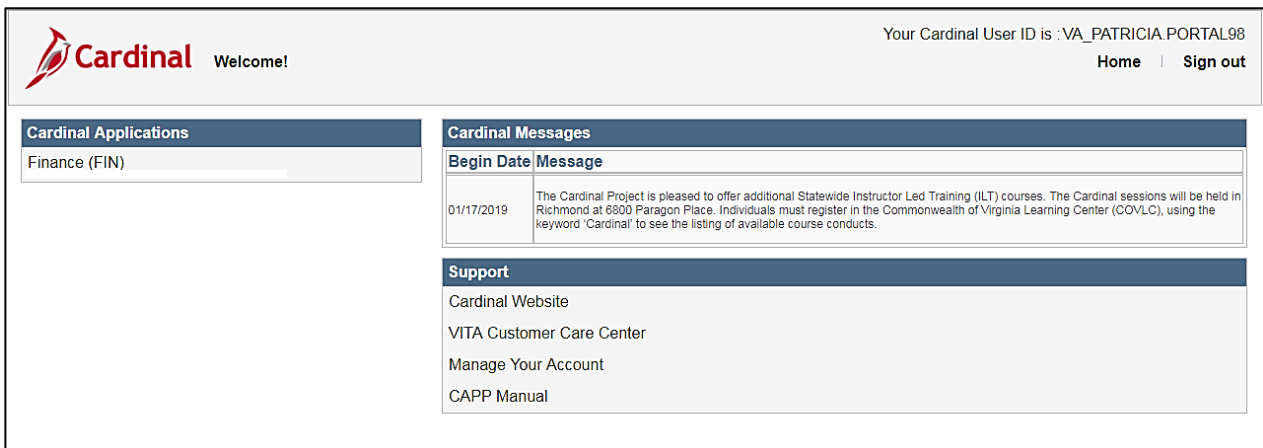


Do not select this option if this is a shared computer/device.

5. The **SMS Authentication** page displays.
6. Click the **Send code** button. The **Send** button changes to **Sent**.
7. Enter the authentication code in the **Enter Code** field on your computer/device.
8. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

Note: If you clear the browser cache on your computer/device, you will need to enter the response again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the response, to have settings added back to the computer/device.

9. Click the **Verify** button to access the **Cardinal Portal**.



Begin Date	Message
01/17/2019	The Cardinal Project is pleased to offer additional Statewide Instructor Led Training (ILT) courses. The Cardinal sessions will be held in Richmond at 6800 Paragon Place. Individuals must register in the Commonwealth of Virginia Learning Center (COVLC), using the keyword 'Cardinal' to see the listing of available course conducts.


10. The **Cardinal Portal** displays.

Setting Up Voice Call Authentication

This additional authentication option allows you to use a mobile or land line to receive an authentication code. After entering your phone number and requesting the code, you will receive a call to the number you entered (land line or mobile). When you answer the call, a voice recording provides the authentication code you need to enter.


Set up multifactor authentication

Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account




Google Authenticator
Enter single-use code from the mobile app.

Setup



SMS Authentication
Enter a single-use code sent to your mobile phone.

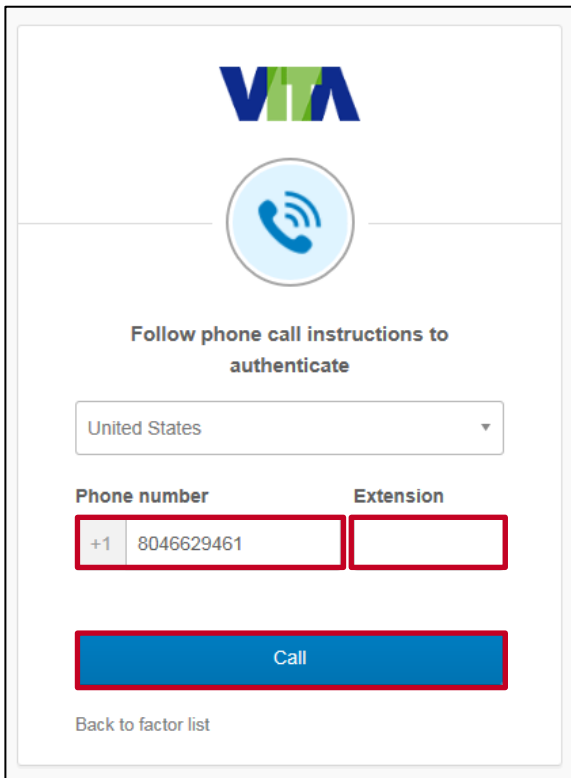
Setup




Voice Call Authentication
Use a phone to authenticate by following voice instructions.

Setup

1. Under **Voice Call Authentication**, click the **Setup** button.



VITA



Follow phone call instructions to authenticate

United States ▼

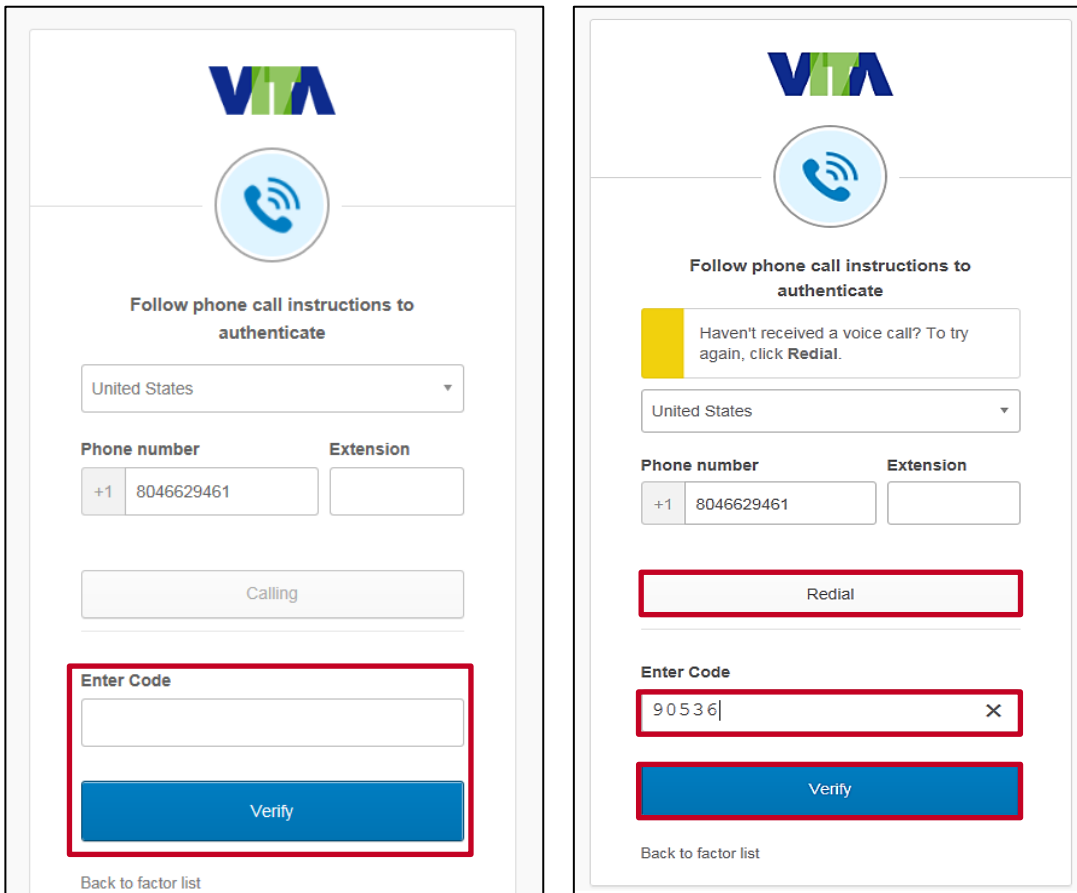
Phone number Extension

+1 8046629461

Call

[Back to factor list](#)

2. The **Follow phone call instructions to authenticate** page displays.
3. Enter the phone number you want to receive the call. The phone number can be either a mobile or land line phone, registered in the United States or Canada.
If the phone requires an extension, enter it in the **Extension** field.
For this scenario, an extension is not added.
4. Click the **Call** button.

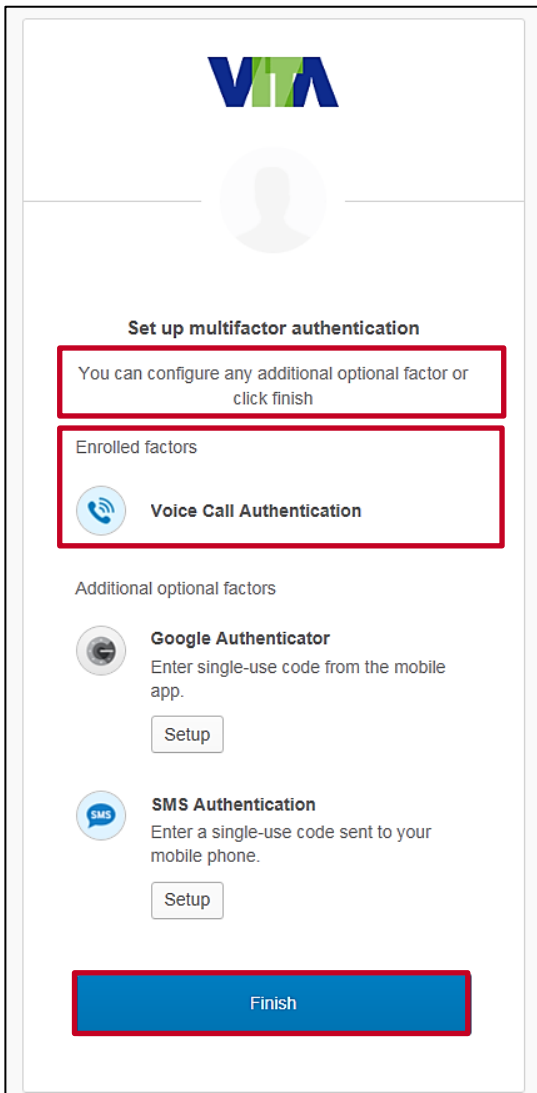


The screenshots show the Cardinal Multi-Factor Authentication interface. The left screenshot shows the initial setup with a 'Calling' button and an 'Enter Code' field. The right screenshot shows the 'Redial' button and the 'Enter Code' field with the code '90536' entered.

5. An **Enter Code** field and **Verify** button display on the page.

Note: The **Call** field changes to **Calling** when the call is in process and **Redial** after the call has disconnected. A message displays “**Haven’t received a voice call? To try again, click Redial.**”

6. A call is made to the number you entered. When you answer the call, a voice recording says: “**Hello. Thank you for using our phone verification system. Your code is XXXXX. Once again your code is XXXXX. Goodbye.**” The call then disconnects.
7. Make note of the authentication code.
8. Enter the authentication code in the **Enter Code** field on your computer/device.
9. Click the **Verify** button.



Set up multifactor authentication

You can configure any additional optional factor or click finish

Enrolled factors

Voice Call Authentication

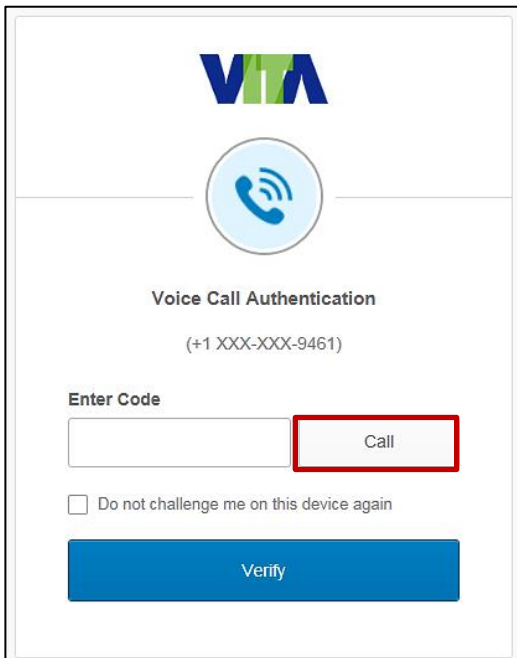
Additional optional factors

Google Authenticator
Enter single-use code from the mobile app.
Setup


SMS Authentication
Enter a single-use code sent to your mobile phone.
Setup

Finish

10. The **Set up multifactor authentication** page displays. A message indicates **You can configure additional optional options or click finish**.
11. The authentication option you selected displays under the **Enrolled factors** section of the page.
Note: If you are using Chrome, you will see a green checkmark next to your enrolled factor.
12. Click the **Finish** button. Now that you have completed your authentication setup, you will be required to authenticate again to log into the **Cardinal Portal**.



VITA



Voice Call Authentication

(+1 XXX-XXX-9461)

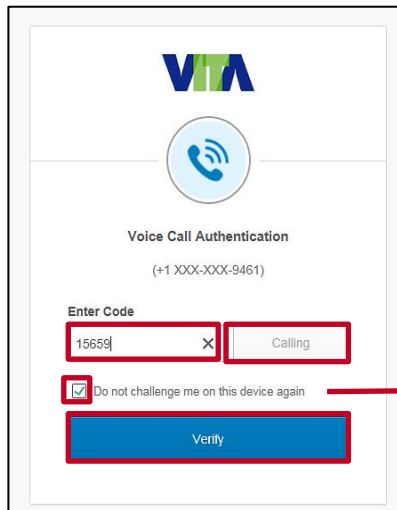
Enter Code

Call

☐ Do not challenge me on this device again

Verify

13. The **Voice Call Authentication** page displays on your computer/device.
14. Click the **Call** button to receive a new authentication code.



Do not select this option if this is a shared computer/device.

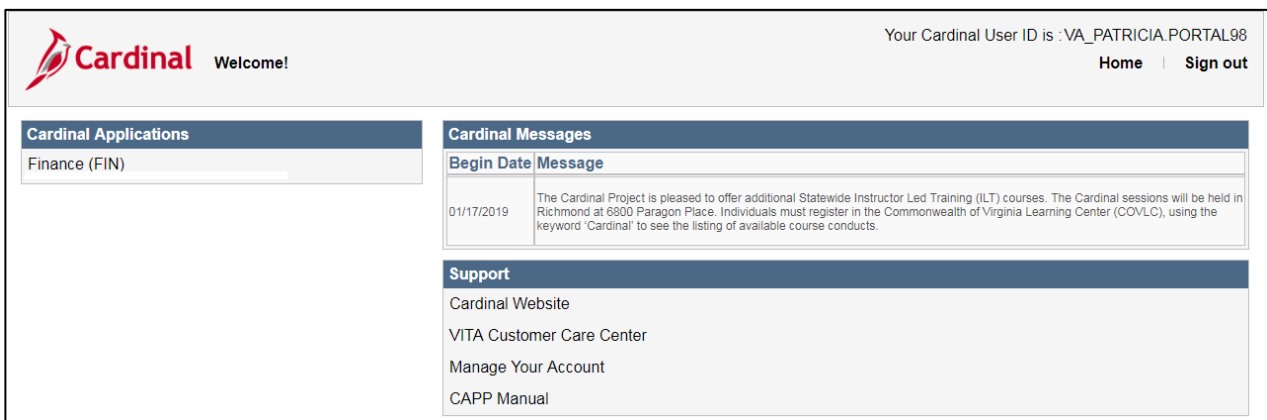
15. Once you receive the call, enter the authentication code in the **Enter Code** field on your computer/device.

Note: The **Call** field changes to **Calling** when the call is in process and **Redial** after the call has disconnected.

16. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

Note: If you clear the browser cache on your computer/device, you will need to enter the authentication code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the authentication code, to have settings added back to the computer/device.

17. Click the **Verify** button to access the **Cardinal Portal**.



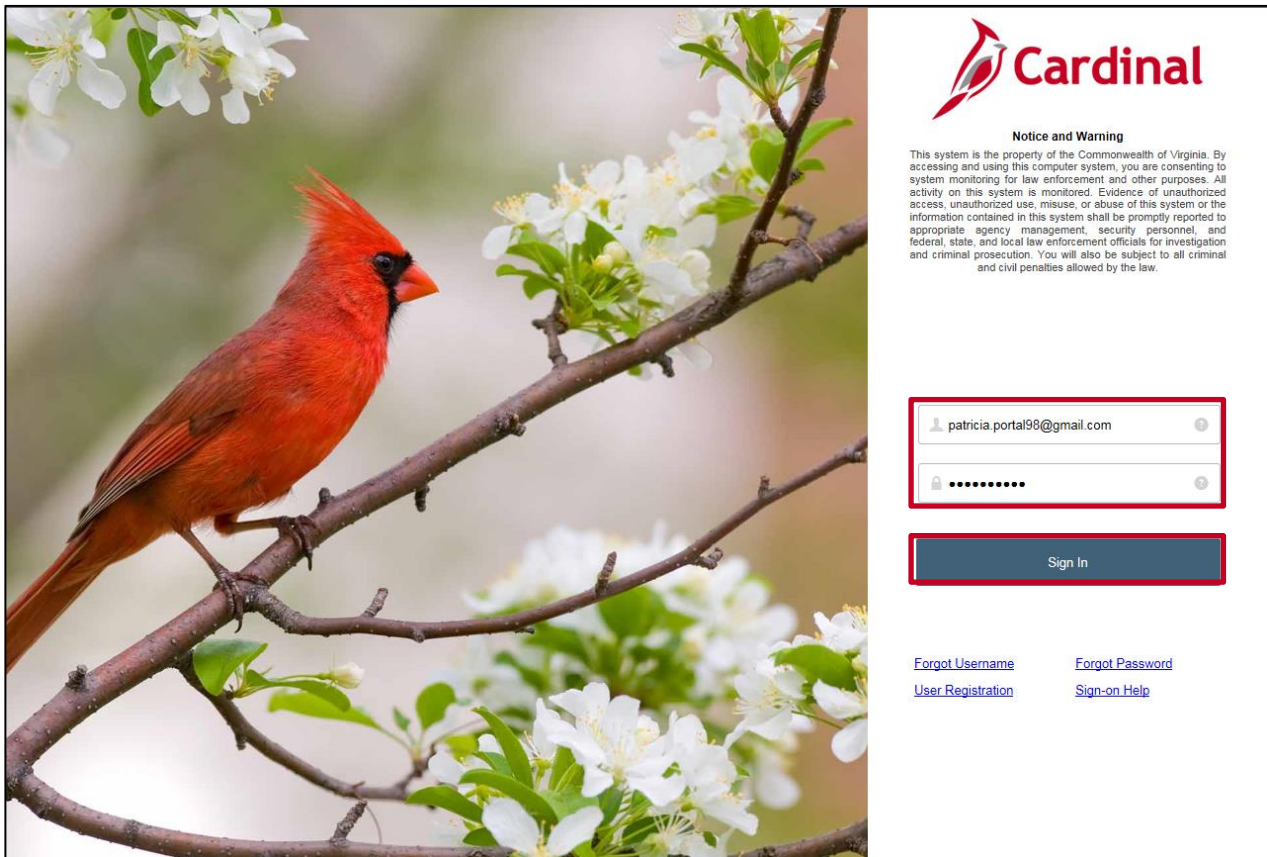
Begin Date	Message
01/17/2019	The Cardinal Project is pleased to offer additional Statewide Instructor Led Training (ILT) courses. The Cardinal sessions will be held in Richmond at 6800 Paragon Place. Individuals must register in the Commonwealth of Virginia Learning Center (COVLC), using the keyword 'Cardinal' to see the listing of available course conducts.

18. The **Cardinal Portal** displays.

Logging in After Setting up Voice Call Authentication

The next time you use the same computer/device to log in to the **Cardinal Portal**, the authentication option you selected is retained.

1. Start by entering the following URL in your computer browser: my.cardinal.virginia.gov.



Cardinal

Notice and Warning

This system is the property of the Commonwealth of Virginia. By accessing and using this computer system, you are consenting to system monitoring for law enforcement and other purposes. All activity on this system is monitored. Evidence of unauthorized access, unauthorized use, misuse, or abuse of this system or the information contained in this system shall be promptly reported to appropriate agency management, security personnel, and federal, state, and local law enforcement officials for investigation and criminal prosecution. You will also be subject to all criminal and civil penalties allowed by the law.

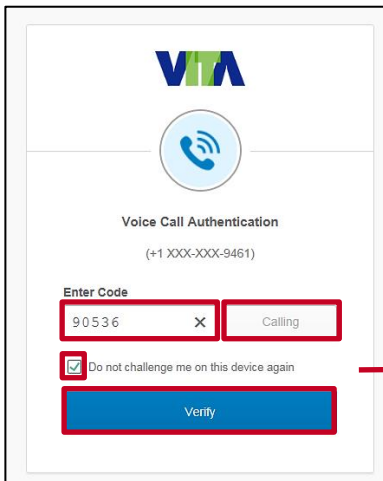
patricia.portal98@gmail.com

.....

Sign In

[Forgot Username](#) [Forgot Password](#)
[User Registration](#) [Sign-on Help](#)

2. Enter your Cardinal Username in the **Cardinal Username** field.
3. In the **Password** field, enter the appropriate password:
 - a. COV users: enter your network password.
 - b. Non-COV users: enter the password you created during the registration process.
4. Click the **Sign In** button.



VITA

Voice Call Authentication
(+1 XXX-XXX-9461)

Enter Code

90536 X Calling

☒ Do not challenge me on this device again

Verify

Do not select this option if this is a shared computer/device.

5. The **Voice Call Authentication** page displays on your computer/device.
6. Click the **Call** button.

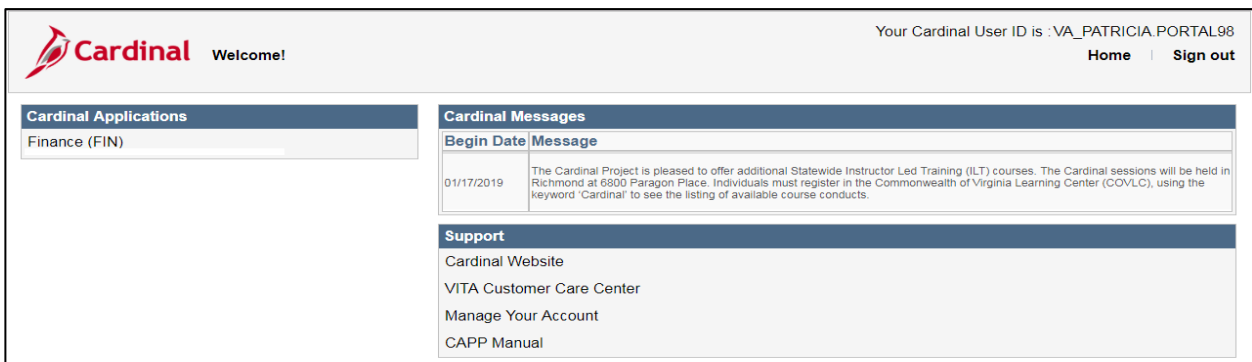
Note: The **Call** field changes to **Calling** when the call is in process and **Redial** after the call has disconnected.

Enter the authentication code after receiving the call in the **Enter Code** field on your computer/device.

7. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

Note: If you clear the browser cache on your computer/device, you will need to enter the authentication code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the authentication code, to have settings added back to the computer/device.

8. Click the **Verify** button to access the **Cardinal Portal**.



Cardinal Welcome! Your Cardinal User ID is : VA_PATRICIA.PORTAL98 [Home](#) | [Sign out](#)

Cardinal Applications	Cardinal Messages				
Finance (FIN)	<table border="1"> <thead> <tr> <th>Begin Date</th> <th>Message</th> </tr> </thead> <tbody> <tr> <td>01/17/2019</td> <td>The Cardinal Project is pleased to offer additional Statewide Instructor Led Training (ILT) courses. The Cardinal sessions will be held in Richmond at 6800 Paragon Place. Individuals must register in the Commonwealth of Virginia Learning Center (COVLC), using the keyword "Cardinal" to see the listing of available course conducts.</td> </tr> </tbody> </table>	Begin Date	Message	01/17/2019	The Cardinal Project is pleased to offer additional Statewide Instructor Led Training (ILT) courses. The Cardinal sessions will be held in Richmond at 6800 Paragon Place. Individuals must register in the Commonwealth of Virginia Learning Center (COVLC), using the keyword "Cardinal" to see the listing of available course conducts.
Begin Date	Message				
01/17/2019	The Cardinal Project is pleased to offer additional Statewide Instructor Led Training (ILT) courses. The Cardinal sessions will be held in Richmond at 6800 Paragon Place. Individuals must register in the Commonwealth of Virginia Learning Center (COVLC), using the keyword "Cardinal" to see the listing of available course conducts.				
	Support Cardinal Website VITA Customer Care Center Manage Your Account CAPP Manual				

9. The **Cardinal Portal** displays.

Appendix


Setting Up Google Authenticator


Since the Cardinal Team is not enabled to support the Google Authenticator app, we do not recommend this option.


Google Authenticator requires you to download the **Google Authenticator** app to your mobile device. The app generates a random token code which changes every 30 seconds. Standard data usage rates apply.

Set up multifactor authentication

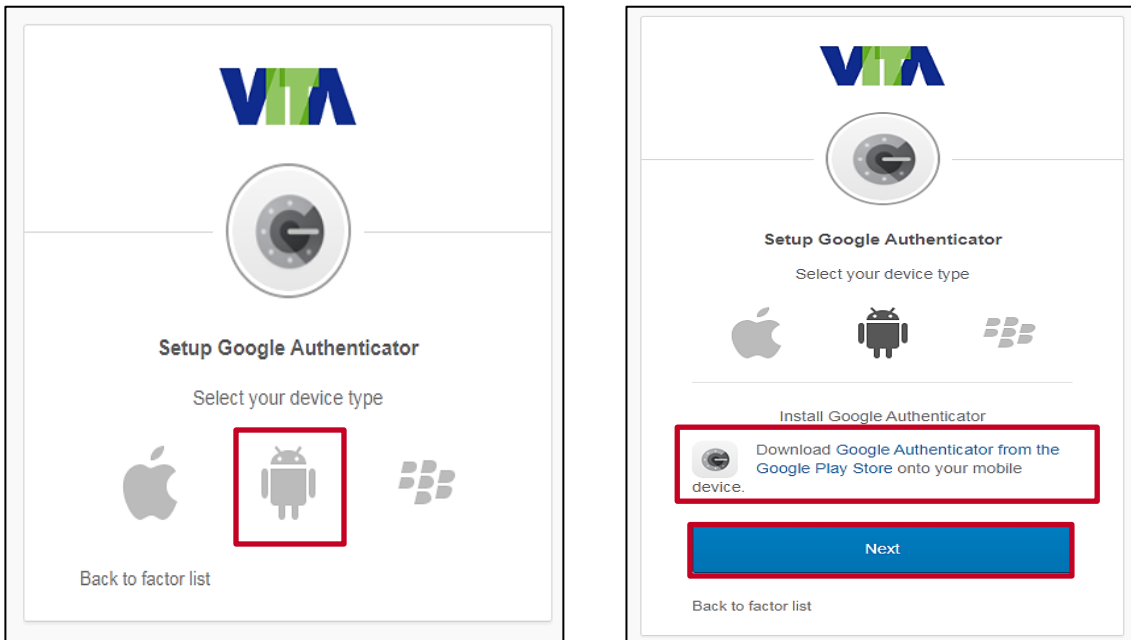
Your company requires multifactor authentication to add an additional layer of security when signing in to your Okta account

**Google Authenticator**
Enter single-use code from the mobile app.
Setup


**SMS Authentication**
Enter a single-use code sent to your mobile phone.
Setup

**Voice Call Authentication**
Use a phone to authenticate by following voice instructions.
Setup

1. Under **Google Authenticator**, click the **Setup** button.



2. The **Setup Google Authenticator** page displays. Click the image for the type of mobile device you want to set up:

- a.  : Apple
- b.  : Android
- c.  : BlackBerry

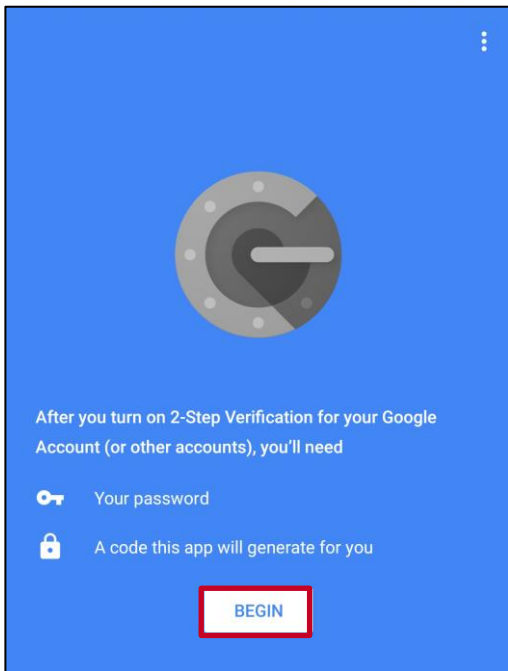
Note: If you do not have one of these mobile devices, click the **Back to factor list** link to return and choose another method for authentication.

3. After you select your device type, a Download message displays. Search for the **Google Authenticator** app (it is free) on your mobile device:

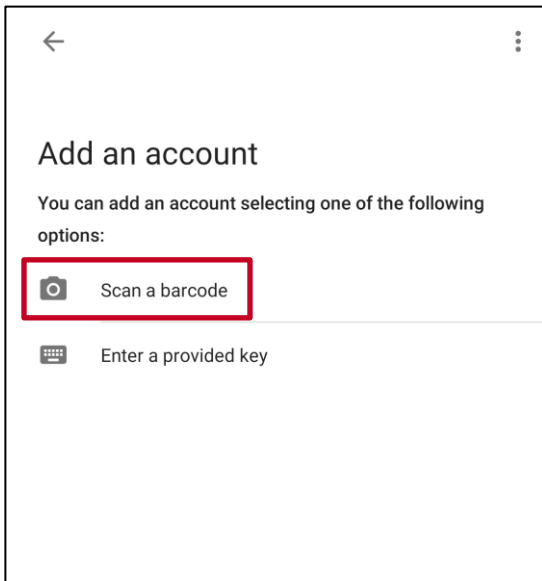
- a. Apple: go to the App Store
- b. Android: go to the Playstore
- c. BlackBerry: go to the World Store

4. Once you locate the app on your mobile device, install and open the app on your mobile device.

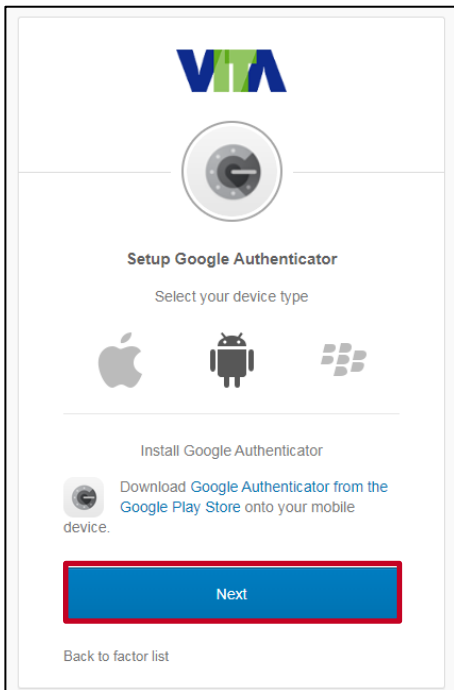
Note: Screens may vary based on mobile device type. These screenshots are based on Android.



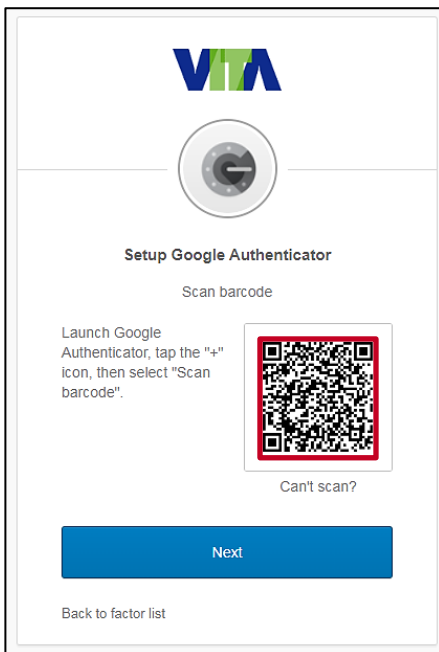
5. The **Google Authenticator** app displays on your mobile device. Click the **BEGIN** button.



6. A page like the one above displays on your mobile device.
7. Select the **Scan barcode** option. This opens the camera on your mobile device.

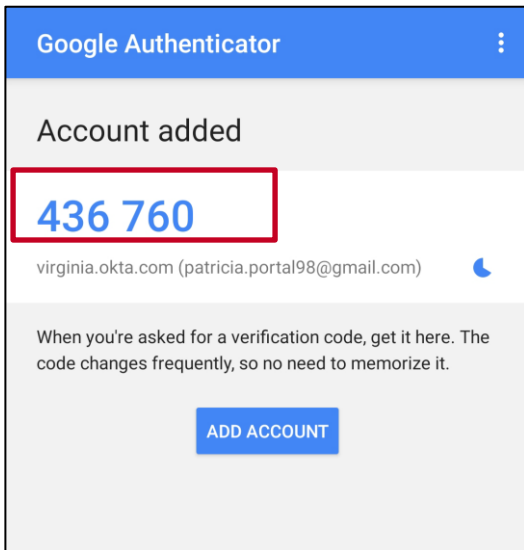


8. On your computer/device screen, click the **Next** button.



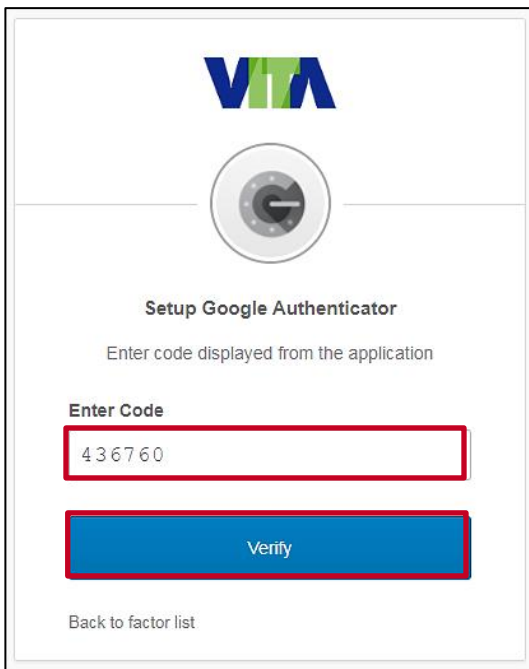
9. The **Setup Google Authenticator** page displays on your computer/device. Point the camera of your mobile device at the barcode.

Note: If the barcode does not scan, follow the instructions in the [Bar Code – Can't Scan](#) section of this job aid.

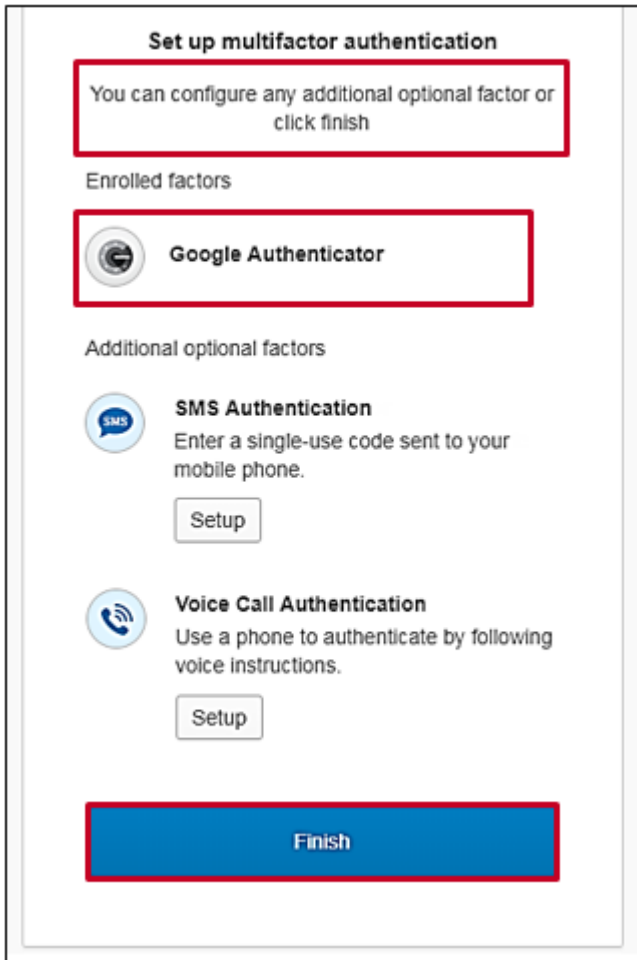


10. The **Google Authenticator** app on your mobile device recognizes the user account and displays a random token code.

Note: The token code will change every 30 seconds.




11. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
12. Click the **Verify** button.




Set up multifactor authentication


You can configure any additional optional factor or click finish

Enrolled factors

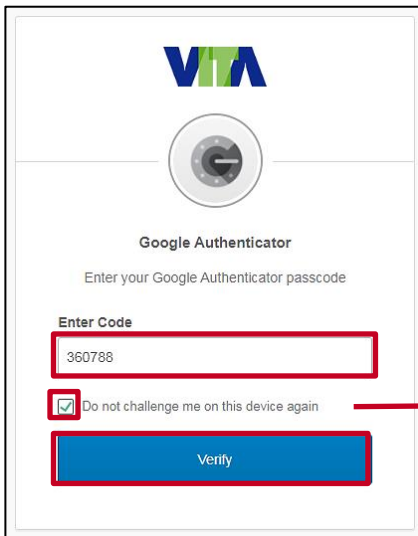
 **Google Authenticator**

Additional optional factors

 **SMS Authentication**
Enter a single-use code sent to your mobile phone.

 **Voice Call Authentication**
Use a phone to authenticate by following voice instructions.

13. The **Set up multifactor authentication** page displays. A message indicates **You can configure any additional optional factor or click finish**.
14. The authentication option you selected displays under the **Enrolled factors** section of the page.
Note: If you are using Chrome, you will see a green checkmark next to your enrolled factors.
15. Click the **Finish** button. Now that you have completed your authentication setup, you will be required to authenticate again to log into the **Cardinal Portal**.

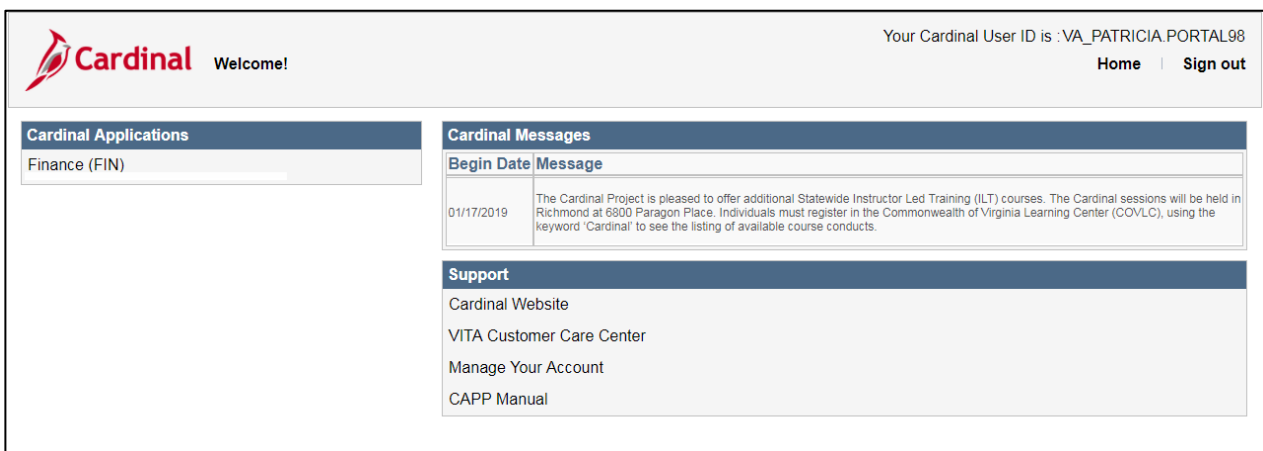


Do not select this option if this is a shared computer/device.

16. The **Google Authenticator** page displays on your computer/device.
17. Open the **Google Authenticator** app on your mobile device.
18. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
19. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

Note: If you clear the browser cache on your computer/device, you will need to enter the token code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the token code, to have settings added back to the computer/device.

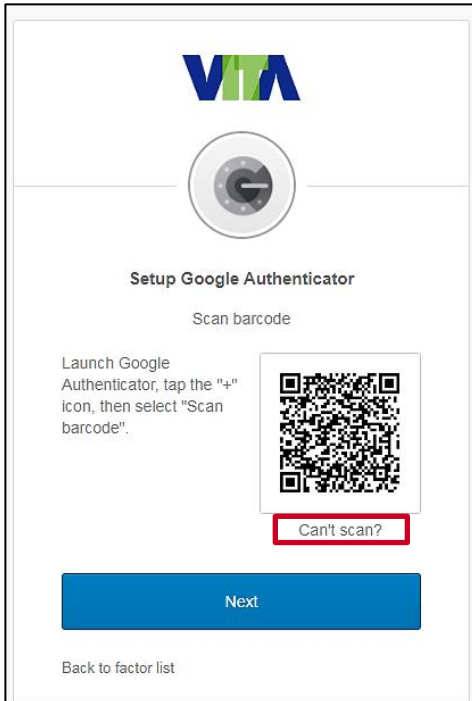
20. Click the **Verify** button to access the **Cardinal Portal**.



21. The **Cardinal Portal** displays.

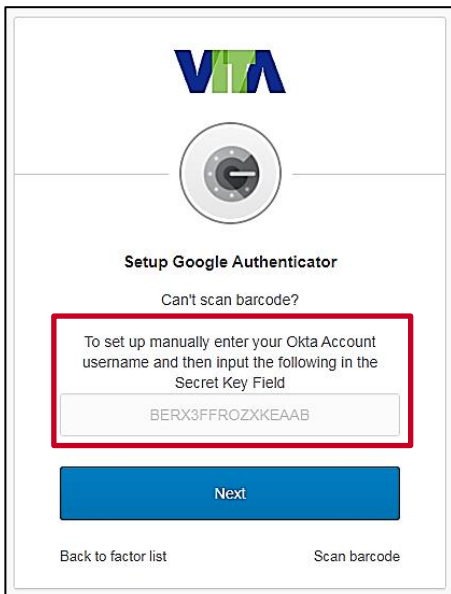
Barcode – Can't scan

If your mobile device is unable to scan the barcode, follow the steps below:



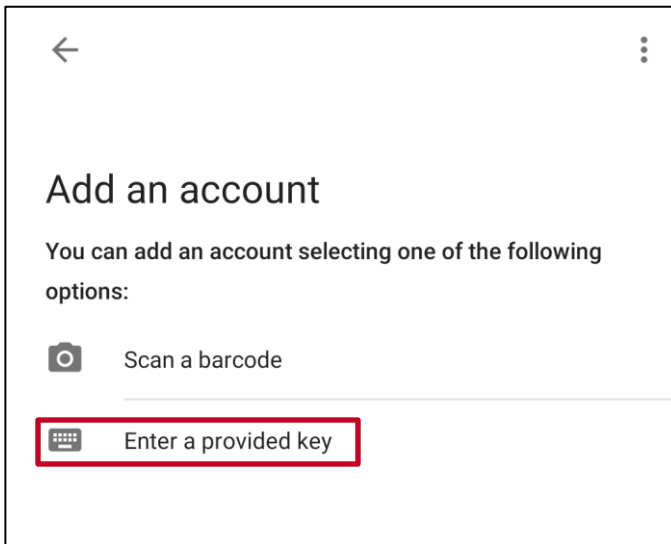
The screenshot shows the 'Setup Google Authenticator' page. At the top is the VITA logo. Below it is a circular icon with a 'G'. The text 'Setup Google Authenticator' is centered. Below that is 'Scan barcode'. To the left, instructions say: 'Launch Google Authenticator, tap the "+" icon, then select "Scan barcode".' To the right is a QR code. Below the QR code is a red-bordered link that says 'Can't scan?'. At the bottom is a large blue 'Next' button. In the bottom left corner is a link that says 'Back to factor list'.

1. Click the **Can't scan?** link on your computer/device.

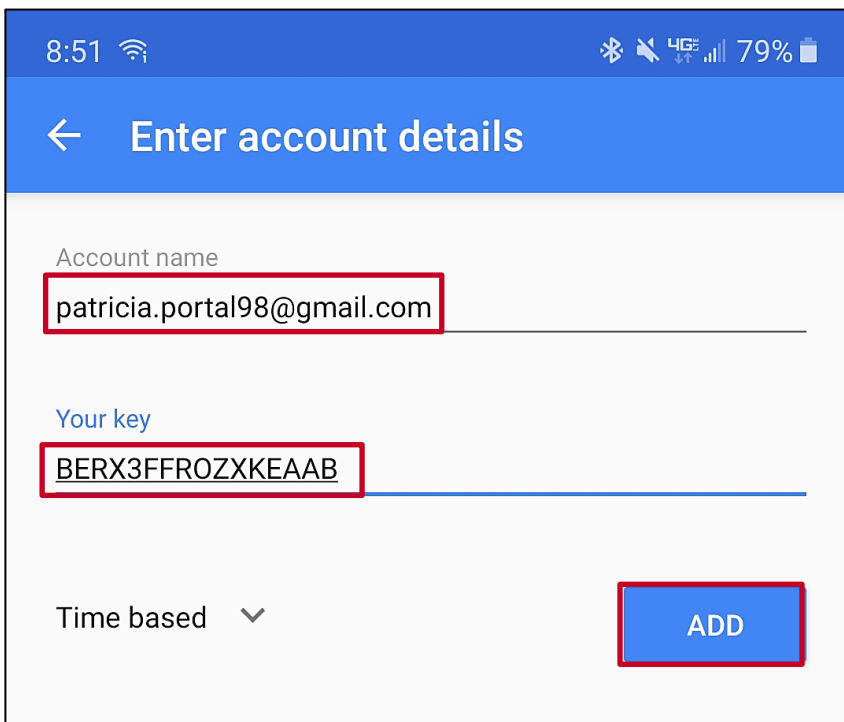


The screenshot shows the 'Setup Google Authenticator' page after clicking the 'Can't scan?' link. The text 'Can't scan barcode?' is centered. Below it, a red-bordered box contains the text: 'To set up manually enter your Okta Account username and then input the following in the Secret Key Field'. Below this text is a text input field containing the secret key: 'BERX3FFROZXKEAAB'. At the bottom is a large blue 'Next' button. In the bottom left corner is a link that says 'Back to factor list'. In the bottom right corner is a link that says 'Scan barcode'.

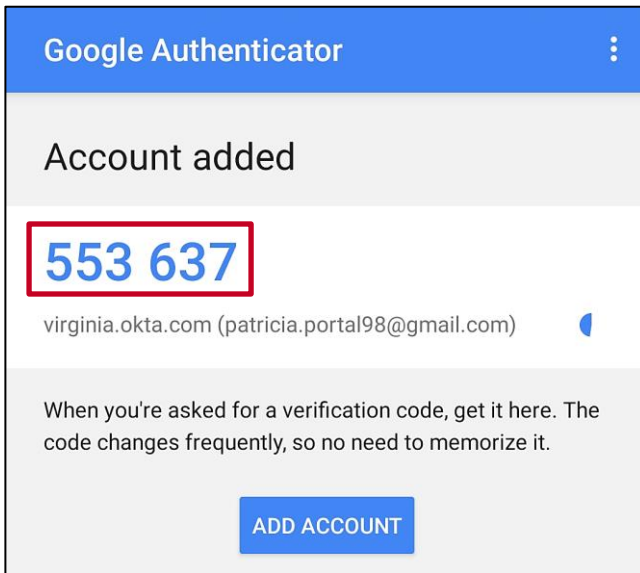
2. The **Setup Google Authenticator** page displays on your computer/device. Follow the instructions on this page to enter the information on your mobile device.



3. On your mobile device, select the **Enter a provided key** option.

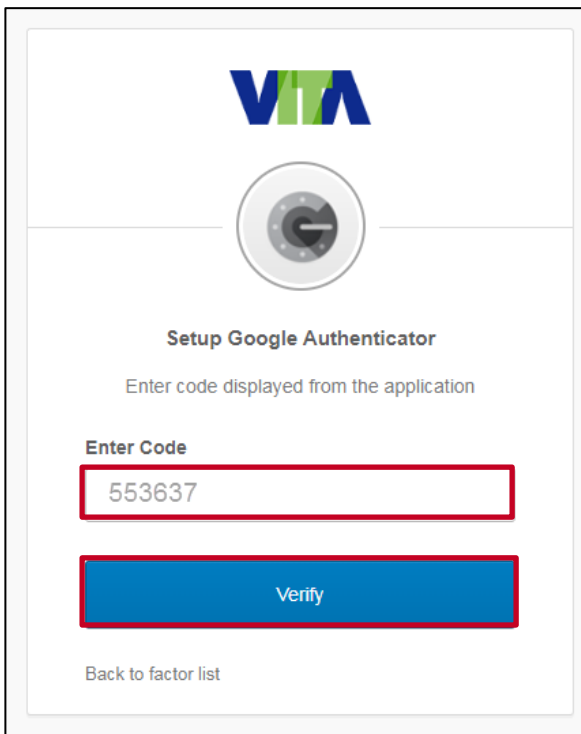


4. On your mobile device, the **Enter account details** page displays. Enter the following as noted below:
- Account name:** Enter your Cardinal Username
 - Your key:** Enter the code that was provided on your **Google Authenticator** page on the computer/device.
5. Click the **ADD** button.

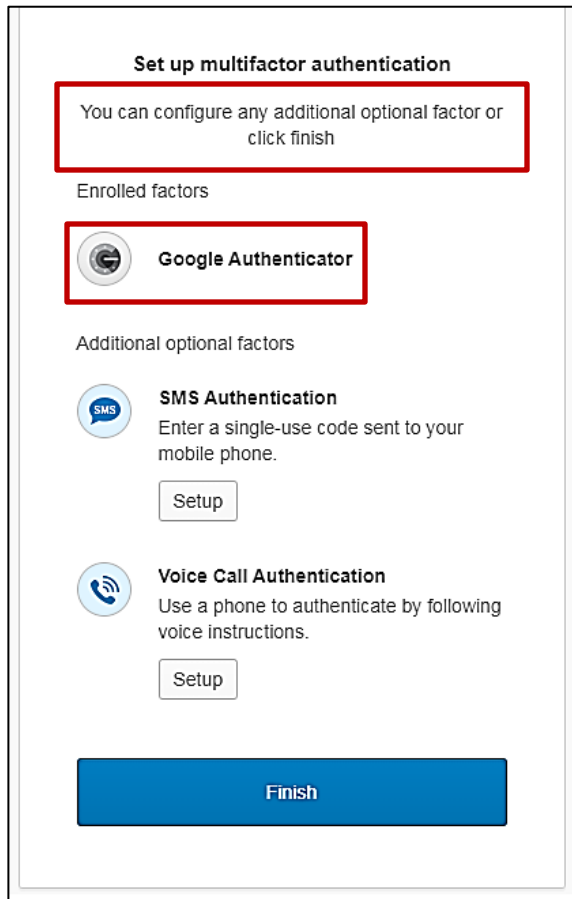


6. The **Google Authenticator** app on your mobile device opens the **Account added** page.
7. The token code displays.

Note: This code changes every 30 seconds.




8. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
9. Click the **Verify** button.




Set up multifactor authentication


You can configure any additional optional factor or click finish

Enrolled factors

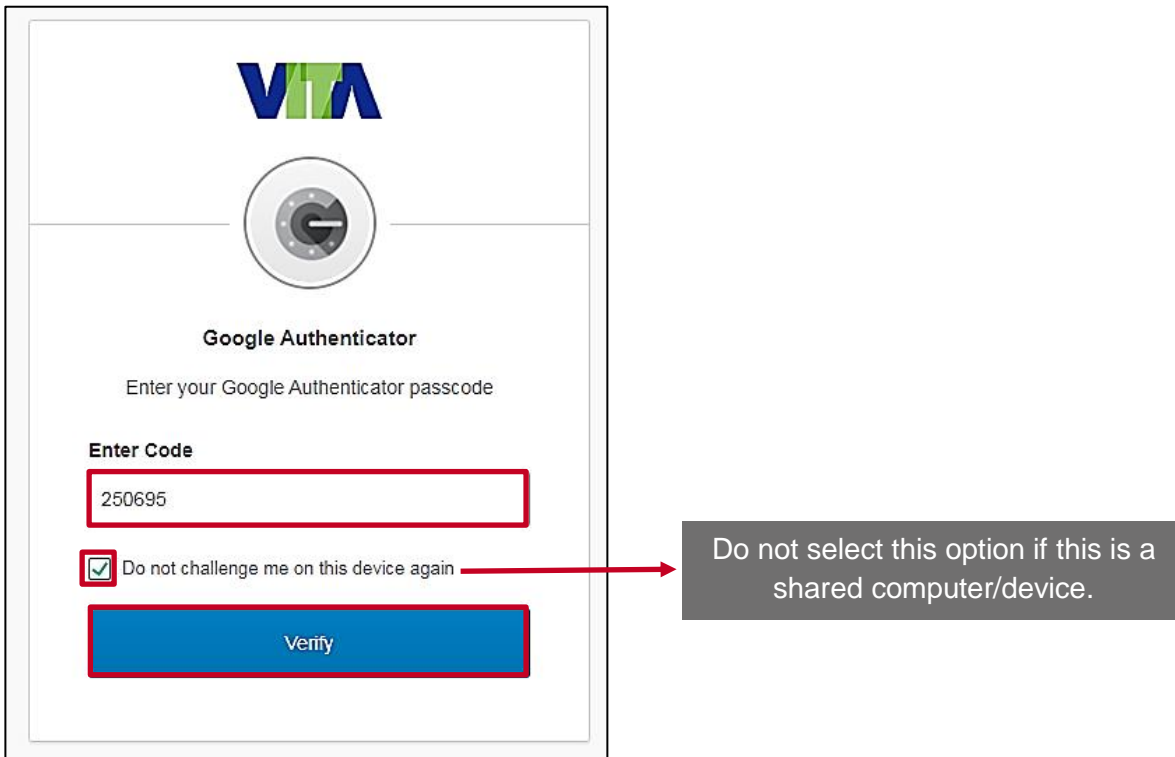
 **Google Authenticator**

Additional optional factors

 **SMS Authentication**
Enter a single-use code sent to your mobile phone.

 **Voice Call Authentication**
Use a phone to authenticate by following voice instructions.

10. The **Set up multifactor authentication** page displays. A message indicates **You can configure any additional optional factor or click finish**.
11. The authentication method you selected displays under the **Enrolled factors** section of the page.
Note: If you are using Chrome, you will see a green checkmark next to your enrolled factors.
12. Click the **Finish** button. Now that you have completed your authentication setup, you will be required to authenticate again to log into the **Cardinal Portal**.



13. The **Google Authenticator** page displays on your computer/device.
14. Open the **Google Authenticator** app on your mobile device.
15. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
16. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

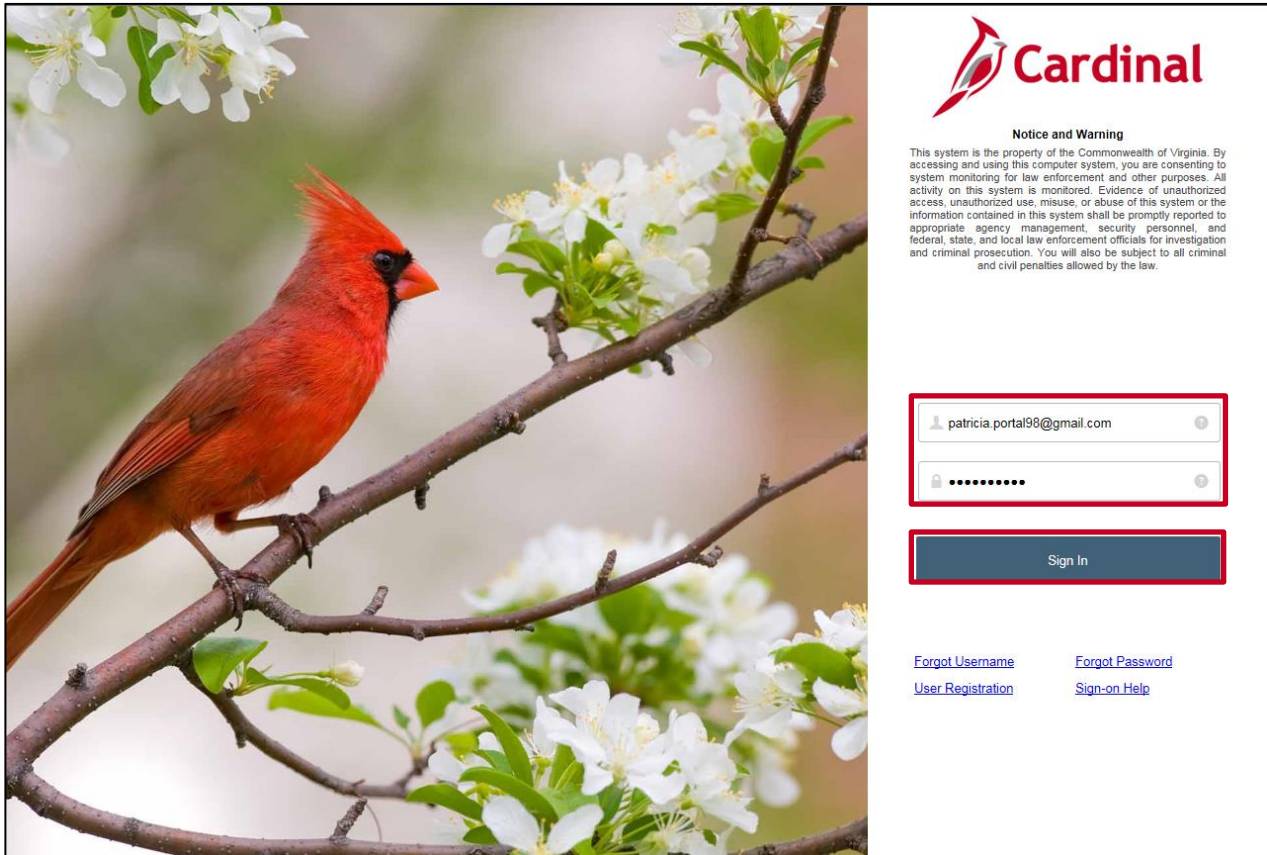
Note: If you clear the browser cache on your computer/device, you will need to enter the token code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the token code, to have settings added back to the computer/device.

17. Click the **Verify** button to access the **Cardinal Portal**.

Logging in After Setting up Google Authenticator

The next time you use the same computer/device to log in to the **Cardinal Portal**, the authentication option you selected is retained.

1. Start by entering the following URL in your computer browser: my.cardinal.virginia.gov.



Cardinal

Notice and Warning

This system is the property of the Commonwealth of Virginia. By accessing and using this computer system, you are consenting to system monitoring for law enforcement and other purposes. All activity on this system is monitored. Evidence of unauthorized access, unauthorized use, misuse, or abuse of this system or the information contained in this system shall be promptly reported to appropriate agency management, security personnel, and federal, state, and local law enforcement officials for investigation and criminal prosecution. You will also be subject to all criminal and civil penalties allowed by the law.

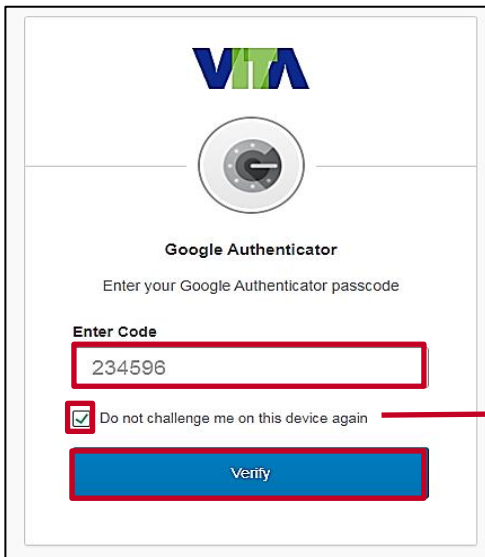
patricia.portal98@gmail.com

.....

Sign In

[Forgot Username](#) [Forgot Password](#)
[User Registration](#) [Sign-on Help](#)

2. Enter your Cardinal Username in the **Cardinal Username** field.
3. In the **Password** field, enter the appropriate password:
 - a. COV users: enter your network password.
 - b. Non-COV users: enter the password you created during the registration process.
4. Click the **Sign In** button.

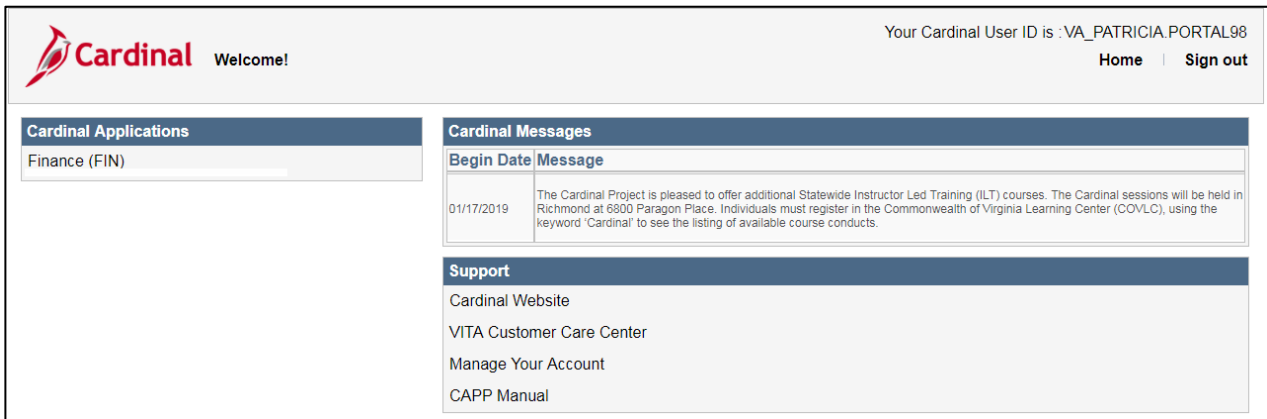


Do not select this option if this is a shared computer/device.

5. The **Google Authenticator** page displays on your computer/device.
6. Open the **Google Authenticator** app on your mobile device.
7. Enter the token code that displays on your mobile device in the **Enter Code** field on your computer/device.
8. To skip this step in the future, select the **Do not challenge me on this device again** checkbox. VITA remembers the computer/device so that MFA verification is not required on subsequent logins. The next time you log in from the computer/device, VITA will skip this step and open the **Cardinal Portal**.

Note: If you clear the browser cache on your computer/device, you will need to enter the token code again. Clearing the browser cache removes the previous settings which allowed the device to be remembered. Check the **Do not challenge me on this device again** checkbox, after entering the token code, to have settings added back to the computer/device.

9. Click the **Verify** button to access the **Cardinal Portal**.



10. The **Cardinal Portal** displays.